システム要求と形式仕様のやわらかい設計支援環境とその試作

2R－5

福沢 尚司* 宋 国煥* 高橋 薫† 神長 裕明‡ 白鳥 則郎*

*東北大学電気通信研究所 / 情報科学研究科, †仙台電波工業高等専門学校, ‡山形大学工学部電子工学科

1 はじめに

システム設計工程における初期段階では，設計対象のシステムに対する機能要求が頻繁に追加・変更される．これら作業は，既に設計済みのシステムの再設計を必要とし，最悪の場合システム全体の再設計を必要とする．

これらの設計作業を支援する一手法として，我々はやわらかい設計支援方法論の構築を目指している．この支援法の特徴は，次の３点にまとめることができる．(1) 命題論理に基づいた機能要求記述法を用いてシステムを機能要求仕様化する．(2) このシステム要求仕様から，合成法を用いて，システムの動作仕様である形式仕様を自動合成する．(3) システム要求が変化した場合，これを合成法に基づいて自動的に形式仕様に反映させる．

現在では，この開発法をより効果的に遂行するため，次の３つの手法に対して研究を行っている．(a) システム要求が含んでいる論理エラーの検証法，(b) 形式仕様上での論理エラー訂正の機能要求仕様への反映法，(c) システム要求と形式仕様の詳細化法．

本稿では，以上の手法を包括的に支援する設計支援環境と，その試作について述べる．

2 準備

2.1 やわらかい設計支援 [3]

本稿ではやわらかい設計支援を次のような性質を持つものとして定義する．(1) 要求の変化した部分に関する設計の部分的変更を行なえる．(2) あいまいな要求から正しく形式仕様を獲得できる．(3) 徐々に要求を具体化しつつ設計を行なう段階的設計ができる．

これらの性質を実現するために，以下のようなシステム要求と形式仕様の表現を構成した．

2.2 システム要求

システムの要求は，(1) 機能要求仕様の集合，(2) 初期条件，(3) 最終条件の集合からなる．ここで，機能要求仕様とは，

$$id : f_{in} \overset{i/o}{\Rightarrow} f_{out}$$

の形式を持ち，入力 i により，命題論理式 f_{in} が成立する状態から，出力 o をともなって，命題論理式 f_{out} が成立する状態に移行することを表す．id は機能要求名である．初期条件，最終条件はそれぞれシステムがその初期および最終状態において満たしているべき命題論理式である．

2.3 形式仕様

命題論理式を状態名，機能要求仕様の入出力をラベルに持つ状態遷移システムであり，設計対象システムの動作仕様である．

3 試作システム

3.1 システム構成

図１に試作した設計支援環境の構成を示す．ユーザは図の上位３つの機器とのやりとりを通して，形式仕様，およびそれと対応するシステム要求を設計する．

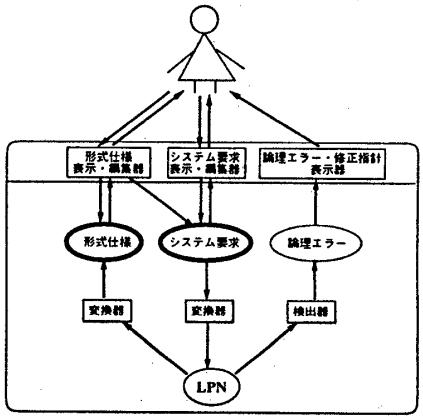

図１ システム要求と形式仕様のやわらかい設計支援環境

ユーザはシステム要求を入力し，それが変換されて形式仕様となって，画面に図として表示されるのを見ながら，システム要求または表示された形式仕様に変更を加えていく形で設計を行なう．その際，論理エラーと，その修正指針が表示されれば，それを助けとして設計に変更を加えることができる．

以下，システムを構成する部品を，ユーザとやりとりを行なう各機器，続いてその他の各機器の順に説明する．

3.2 システム要求表示・編集器

ユーザは入力用インタフェースを通して，システム要求を入力する．まず必要な数の命題論理変数，入力・出力の記号を入力して，次にそれらを部品として，機能要求仕様，初期条件，最終条件を入力する．機能要求と最終条件は複数入力可能である．部品が不足したり，不用になっりしたら，前段階に戻ることもできる．さらに，命題論理変数間の依存関係（例えば，A が成立する時

A Flexible Design Support Environment for System Requirements and Formal Specifications, and Its Prototyping

Shoji Fukuzawa*, Kukhwan Song*, Kaoru Takahashi†, Hiroaki Kaminaga‡ and Norio Shiratori*

*{Reseach Institute of Electrical Communication, Graduate School of Information Sciences} Tohoku Univ. † Sendai National College of Technology ‡ Faculty of Engineering, Yamagata Univ.

には，B と C が成立しなければならない．）を設定することが可能で，これを利用してより自然な設計を行なうことができる．

機能要求仕様を用いることで，システムに要求される各機能毎に独立した記述が可能であり，追加，消去，修正が容易に行なえる．

システム要求入力前に命題論理式の制限を入力することで，その条件が満たされる場合に限定されたシステム要求を記述できる．これにより，抽象的なシステム要求を段階的に詳細化して獲得できる．

3.3 形式仕様表示・編集器

形式仕様を図として表示し，状態や遷移の位置を自由に変更して記録することが可能である．ラベル位置調整，拡大・縮小等が可能であり，PostScript 形式のファイル出力機能を有していて，プリンタに出力することもできる．図2 に形式仕様の PostScript 形式ファイル出力例を示す．

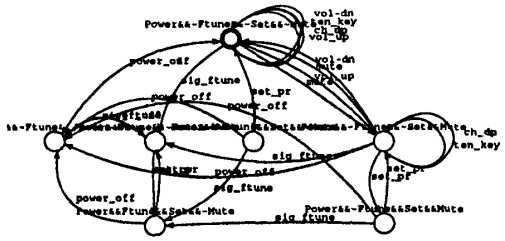

図2 形式仕様の PostScript 形式ファイル出力例

また，このとき図として表示された形式仕様に直接編集を加えることが可能である．編集結果は形式仕様と，元となったシステム要求に自動的に反映させることができる．この機能により，視覚的にわかりやすい編集が可能である．システム要求の編集機能と併用することで，わかりやすい，また効率的な設計を行なえる．

3.4 論理エラー・修正指針表示器

これは，検出された論理エラーの種類に応じ，その修正のための指針をユーザに示す．示されるのは，エラーの原因となっている遷移や状態と，それに対する適切な処理の候補である [3]．そのため，修正作業に対し，形式仕様表示・編集器の編集機能を用いやすい形式になっている．

3.5 システム要求 →LPN 変換器

これは，システム要求を LPN に変換する．LPN：Logical Petri Net [1, 2] とは，ペトリネットに機能要求仕様を表現するための拡張を行なったものである．システム要求から形式仕様への変換に用いられる．変換アルゴリズムは文献 [1] 参照．

3.6 LPN → 形式仕様変換器

これは，LPN を形式仕様に変換する．これは，ペトリネットの性質を利用した変換法を実装したものであり，その過程で得られる情報は，論理エラー検出に利用される．変換アルゴリズムは文献 [1] 参照．

3.7 論理エラー検出器

これは，LPN から形式仕様への変換過程で得られる状態への可達情報をもとに，論理エラーを検出する．検出法に関しては文献 [2] 参照．検出可能な論理エラーは，(1) 最終条件の充足不能，(2) デッドロック，(3) 実行されない機能，(4) 無限ループの 4 種類である．

4 実行画面

図3 に実行画面を示す．

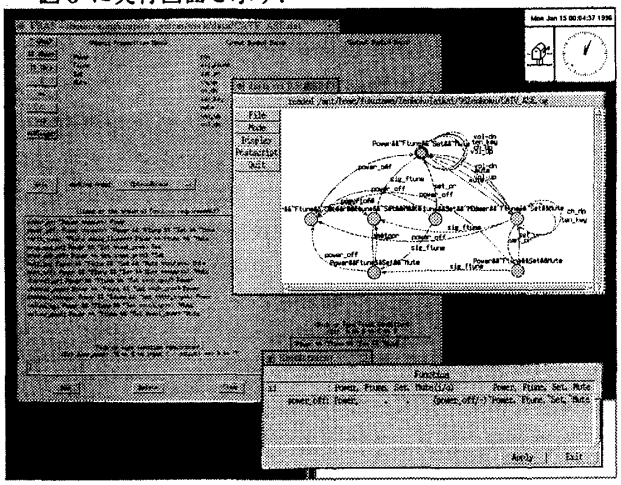

図3 実行画面

X Window 上にシステム要求と形式仕様それぞれの表示・編集器があり，必要に応じてそれぞれのサブウィンドウや論理エラーとその修正指針を表示するウィンドウが開くようになっている．

5 まとめ

本稿ではシステム要求と形式仕様の設計のための支援環境の構成を示し，その試作について述べた．

今後の課題として，(1) 編集や詳細化の機能の追加，(2) システム要求の再利用・データベース化，(3) 実装システム上での試験・評価が挙げられる．

参考文献

[1] 宋 国煥，富樫 敦，白鳥 則郎，論理ペトリネットを用いた形式仕様の自動変換と検証，信学技報，*Tech. Rep. of IEICE*, CST94-29, pp.101-108 (1994).

[2] 宋 国煥，富樫 敦，白鳥 則郎，Verification and Refinement for System Requirements, accepted for publication (in Japanese).

[3] K. H. Song, S. Fukuzawa, K. Takahashi, H. Kaminaga and N. Shiratori, A Flexible Design Support System for Requirement and Formal Specification, 電子情報通信学会，SSE95-67, pp.79-84 (1995).